Statement of Ira Rubinstein, Associate General Counsel

Microsoft Corporation

Testimony Before the House Committee on Energy and Commerce

Hearing on "Combating Spyware: H.R. 29, the 'SPY ACT'"

January 26, 2005

Chairman Barton, Ranking Member Dingell, and Members of the Committee: My name is Ira Rubinstein and I am an Associate General Counsel at Microsoft Corporation. I want to thank you for the opportunity to share with the Committee Microsoft's views on addressing spyware – an issue on which this Committee has been at the forefront. In particular, I want to thank Chairman Barton and Ranking Member Dingell, Representatives Stearns and Schakowsky, the Chairman and Ranking Member, respectively, of the Commerce, Trade, and Consumer Protection Subcommittee, and Representatives Bono and Towns, the lead Republican and Democrat sponsors of H.R. 29, the SPY ACT. This Committee has worked tirelessly to raise public awareness of the threat posed by spyware, and to draft legislation that is carefully targeted to address the bad behavior at the root of the problem – without unnecessarily impacting legitimate software applications. Microsoft believes the Committee has met this goal: we are therefore pleased to support the SPY ACT in its current form, and we look forward to working with Congress as the bill moves forward.

Nine months ago, my colleague Jeffrey Freidberg, who is the Director of Windows Privacy at Microsoft, testified at a hearing of this Committee's Subcommittee on Commerce, Trade, and Consumer Protection on the nature and nuances of spyware, and provided a slide presentation demonstrating some common tricks used by nefarious spyware publishers to deceive users into downloading unwanted programs. He also described Microsoft's commitment to attacking spyware on several levels – technology, consumer education, industry best practices, and enforcement – and the role of legislation in complementing this strategy. Today, I want to tell you about the progress that has

been made in each of these areas over the past nine months, and the ways in which the public and private sectors can continue working together to restore choice and control back where it belongs – in the hands of consumers.

Spyware Remains a Pervasive Problem.

As Chairman Barton aptly recognized at last year's hearing, spyware represents an "unwanted intrusion that is used for purposes that we have not approved, and most of the time without our even knowing it."[1] Purveyors of spyware manipulate computer users through misleading download requests, false icons, and covert practices that trick users or override low security settings in order to install programs that users do not need or want. Unlike legitimate applications, these programs show no respect for users' ability to control their own computers, and they misuse many features that can be an asset with proper disclosure, user authorization, and control. Instead of leading to personalization and better user experiences, these features are manipulated to surreptitiously monitor user activities, hijack home pages, and deliver an unstoppable barrage of pop-up advertisements. In short, spyware is a problem of bad practices – practices that mislead, deceive, or even bully users into downloading unwanted applications.

Spyware continues to be a primary frustration for our customers and industry partners. We receive thousands of calls from customers each month directly related to

---

[1] *Spyware: What You Don't Know Can Hurt You: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce*, 108th Cong. 77 (2004) (statement of Chairman Barton, House Comm. of Energy and Commerce).

deceptive software, and we continue to receive reports that suggest such software is at least partially responsible for approximately one-half of all application crashes that our customers report to us. In addition, industry partners have indicated that unwanted and deceptive software remains one of the top support issues they face, and we understand that it costs many of the large computer manufacturers millions of dollars per year.

Other studies demonstrate the continued growth of the problem. A study last fall conducted by America Online and the National Cyber Security Alliance found that approximately 80 percent of all users had some form of spyware or adware on their machines, and that the average computer contained 93 spyware or adware components.[2] Perhaps most troubling, 89 percent of respondents whose computers had tested positive were unaware that their systems contained any spyware.[3] Over the past year, we have also seen a rise in a particularly disturbing form of spyware programs – so-called "betrayware." These applications claim to be anti-spyware detection or removal programs, but are in fact spyware; some analysts now estimate that there are more than 130 separate betrayware programs lurking in cyberspace.[4]

The explosion in the volume of spyware, and the accompanying increase in the complexity with which those programs operate and the damage that they do, has had an enormous impact on Microsoft. As we explained last year, many of our customers blame

---

[2] *See* AOL/NCSA Online Safety Study (Oct. 2004), *available at* http://www.staysafeonline.info/news/safety_study_v04.pdf.

[3] *Id.*

[4] *See* Eric L. Howes, *The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites, available at* http://www.spywarewarrior.com/ rogue_anti-spyware.htm.

the problems caused by these programs on Microsoft software, believing that their systems are operating slowly, improperly, or not at all because of flaws in our products or other legitimate software. Spyware programs have increased our support costs, harmed our reputation and, most importantly, thwarted our efforts to optimize our customers' computing experiences.

Anti-Spyware Tools Are Enabling Consumers To Take Back Control.

Although spyware is becoming more pervasive and complex, the good news is that there have also been enormous strides over the past year in the fight against spyware – particularly with respect to the development of anti-spyware tools that empower users to protect themselves. As one example, in January of this year, Microsoft launched the Beta version of Windows AntiSpyware – Microsoft's first dedicated anti-spyware tool based on technology developed by GIANT Software Company, Inc. Microsoft acquired this technology from GIANT and rapidly developed and distributed the anti-spyware beta because our customers have made clear that spyware represents a major problem to them, and that they want Microsoft to deliver effective solutions as quickly as possible.

Windows AntiSpyware works by scanning a customer's computer to locate spyware and other known deceptive software threats, and then giving users the tools to easily and rapidly remove those programs – as well as to quickly restore certain damage done by these programs. Once the spyware has been removed, the Windows AntiSpyware Scan Scheduler enables the scheduling of regular scans to help users maintain the condition of their computers. Windows AntiSpyware can also be configured

to block known spyware and other unwanted software from being installed on the computer in the first place. To do this, the program relies on the worldwide SpyNet™ community, which plays a crucial role in determining which suspicious programs are classified as spyware. A voluntary network of users, SpyNet™ helps uncover new threats quickly to ensure that all users are better protected, and any user can choose to join SpyNet™ and report potential spyware to Microsoft. When new spyware programs are confirmed through SpyNet, their unique digital identifiers, or "signatures," can be automatically downloaded by Windows AntiSpyware, helping to stop these new threats before they gain a foothold.

Windows AntiSpyware also provides continuous protection to computers, establishing security checkpoints to guard against more than 50 separate ways that spyware can be downloaded. These checkpoints are monitored by (1) *Internet agents* that help protect against spyware that makes unauthorized connections to the Internet or changes a computer's Internet settings; (2) *system agents* that guard against spyware that makes unauthorized changes to a computer's non-Internet settings (such as passwords or security levels); and (3) *application agents* that protect against spyware that alters applications (such as modifying browsers or launching unwanted programs). If known spyware is detected at these checkpoints, it will be blocked. If an unknown program is detected, Windows AntiSpyware informs the user and asks whether to let the download proceed.

Another feature of Windows AntiSpyware is its ability to work with the security enhancements in Windows XP Service Pack 2 ("XPSP2"). When Mr. Friedberg testified

before the Subcommittee last April, he described a number of ways in which XPSP2 would help block the entry points used by spyware programs by better informing users in advance about the type of software they would be installing. As promised, Microsoft did introduce XPSP2 in 2004, and these enhancements are designed to target the particular tricks that spyware distributors use to surreptitiously install unwanted programs:

- A new pop-up blocker, turned on by default, that reduces a user's exposure to unsolicited downloads;
- A new download blocker that suppresses unsolicited downloads until the user expresses interest;
- Redesigned security warnings that make it easier for users to understand what software is to be downloaded, make it more obvious when bad practices are used, and allow users to choose to never install certain types of software; and
- A new policy that restricts a user's ability to directly select "low" security settings.

Beyond Windows AntiSpyware and XPSP2, Microsoft will continue working collaboratively with all of our security partners: developing anti-spyware tools that empower our customers to protect themselves is a top priority. In the short term, we want everyone to run some kind of anti-spyware solution on a regular basis. In the long term, we want to develop and implement solutions so that spyware is no longer a major issue for our customers. This is an ambitious goal that will require cooperation and dedication, but we believe that the acquisition of GIANT and implementation of Windows AntiSpyware and XPSP2 are significant strides toward achieving that result.

Advances in Education, Enforcement, and Industry Standards Are Evident.

Technology is a critical part of the solution to spyware, but it cannot work alone. Heightened consumer education, aggressive law enforcement, and improved industry self-regulation are also important to ending the spyware epidemic. In the nine months since Microsoft last testified on spyware, there have been significant developments in each of these areas.

Consumer Education. A year or two ago, only the most sophisticated users even knew what spyware was, let alone how to stop it. Now spyware is becoming well-known as a critical consumer protection issue. For example, in its first day on the Microsoft home page, our new Windows AntiSpyware site received more than 130,000 clicks – easily a record for a launch on our home page, and an indication of the tremendously increased customer interest in and attention to the spyware problem.

Much of the credit for heightening consumer awareness about spyware should go to Congress – and particularly to this Committee. Through hearings such as this and determined efforts to enact effective anti-spyware legislation, Congress has attracted media attention to the spyware problem, and has helped educate consumers about the importance of the issue and how to protect themselves. Industry should also play a role in consumer education, and the Web site we launched in 2004 – *www.microsoft.com/spyware* – contains information that is specifically designed to help consumers understand, identify, prevent, and remove spyware. We update this site regularly, and it now includes a comprehensive but easy-to-read white paper describing our spyware strategy, as well as public newsgroups on spyware that our security-focused

"most valuable professionals" monitor to assist the online community. We want to provide users with clear, current, and trusted resources to help understand, remove, and avoid spyware.

Representative Bono emphasized last year that "it is necessary that we [government and industry] collectively educate consumers about the nature and the threats of spyware," and we agree.[5] Although much work has been done over the past year to educate consumers about spyware, we are committed to continuing to working with you and other industry members in this important effort.

Enforcement of Existing Laws. The use of aggressive enforcement actions against spyware purveyors is another critical part of our approach to the problem. Targeting the most insidious violators would have a significant impact on the amount and type of spyware that is produced and distributed – and would serve as a powerful deterrent to would-be violators.

Last April, we explained to the Subcommittee that enforcement actions were possible under existing law. In October 2004, the Federal Trade Commission demonstrated that this was true, taking the first federal enforcement action and obtaining a temporary restraining order against a major distributor of spyware for unfair and deceptive practices that violated the FTC Act. The defendant in that case, Stanford Wallace (who is also known as the "Spam King"), had developed and installed on

---

[5] *Spyware: What You Don't Know Can Hurt You: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce,* 108th Cong. 6 (2004) (statement of Rep. Bono, House Comm. of Energy and Commerce).

unsuspecting users' computers code that tracked their Internet behavior, changed home pages and search engines, and launched a stream of pop-up ads. Wallace then went a step further and targeted these users with pop-up advertisements promoting faulty anti-spyware remedies that Wallace sold for approximately $30 each.

Microsoft supported the FTC's investigation in that case, and our Internet Safety Enforcement team is committed to enforcing existing laws against the distributors of spyware. The team investigates spyware threats that are reported by customers or others, working with government and industry partners and using advanced technology to find the sources of these programs. After the investigation, the team either pursues these cases internally or refers them to law enforcement, including the FTC, U.S. Attorneys, and State Attorneys General. And as in the suit against the Spam King, the team also assists law enforcement officials with their spyware investigations. Microsoft believes that the public and private sectors should continue to work together to hold spyware publishers accountable for their unlawful acts, and we look forward to other successful enforcement actions in the future.

Industry Best Practices. Developing a set of industry-wide standards is another piece of our spyware strategy. Such best practices create an incentive for legitimate software publishers to distinguish themselves from bad actors, and can serve as a foundation for programs that certify and label the good actors – which in turn empower users to make informed decisions about the software they download to their computers.

Representatives from a broad range of companies have been working to develop and implement a set of best practices, but more needs to be done. Initial efforts have

focused on standards for the installation of software through the Internet – as well as more broadly with respect to the collection and use of personal information, the display of pop-up advertisements, and the form and substance of notice and consent. The overriding goal of these practices is to empower consumers – allowing them to make informed decisions by providing appropriate notice and consent experiences, balancing the need for transparency and detail, and offering appropriate controls. Self-regulatory measures should continue to evolve to account for the complexities and challenges that are a result of the ever-changing nature of technology. Microsoft is committed to working with industry to formulate best practices and believes that these practices can help supplement other efforts.

Targeted Legislation Has a Role To Play.

Microsoft is optimistic that this combination of technology, education, enforcement, and industry standards can effectively combat the spyware problem. And significant progress has been made toward this goal in the past year: technological solutions to empower consumers to protect themselves from spyware are now widely available; consumers are much more educated about the nature and scope of spyware; a successful enforcement action has been taken against a spyware publisher under existing law; and legitimate industry practices are becoming better and more consistent.

Federal legislation can be an effective complement to this strategy, providing an additional layer of protection for consumers and another tool for enforcement officials. As we stressed at the beginning of this process, however, Congress must proceed

cautiously to ensure that such legislation targets the deceptive behavior of spyware publishers – and not features or functionalities that have substantial legitimate uses. This distinction is critical to avoid imposing unworkable requirements on legitimate applications and adversely affecting legions of computer users.

The Proposed Legislation Has Improved Dramatically.

When we last testified, we offered some scenarios in which well-intended legislation could have unfortunate and unintended consequences. As you know, we were concerned that initial drafts of anti-spyware legislation contained provisions that might compromise specific functionalities rather than target the bad practices at the core of the spyware problem. We have been extremely pleased, however, at the willingness of Representatives Bono and Towns and other members of this Committee to work with us and others in the private sector to create a bill that captures the bad actors without unnecessarily impeding the good ones. Representative Towns recognized this when the SPY ACT was brought to the House floor last year, noting that "any time we legislate on highly technical matters, there is always a danger in stifling innovation or making the use of legitimate software too burdensome. It is a very difficult tightrope to walk, but I think we have done an excellent job in walking that line."[6] That we successfully worked together to achieve this balance is apparent when we re-examine those scenarios we raised last April.

[6] 150 Cong. Rec. H8085 (daily ed. Oct. 5, 2004) (statement of Rep. Towns).

Disruptive User Experience. As we explained then, many legitimate software programs contain an information-gathering functionality that these programs need in order to perform properly. These include error reporting applications, troubleshooting and maintenance programs, security protocols, and Internet browsers. Imposing notice and consent requirements every time these legitimate programs collect and transmit a piece of information would disrupt the computing experience, because users would be flooded with constant, non-bypassable warnings – making it impossible to perform routine Internet functions (such as connecting to a web page) without intolerable delay and distraction.

The current version of the SPY ACT understands these issues, and takes steps to safeguard the user experience. In particular, the bill allows notices to consumers to be tailored to take into account different scenarios. It also contains important exceptions for critical functionalities – such as security procedures and authentication checks – and recognizes circumstances where information-sharing is driven by the user. These revisions help the legislation target bad actors without impeding legitimate applications.

Compromised Consent Experience. We were also concerned about "one size fits all" notice and consent requirements, which may not give users sufficient context to make informed decisions. For example, requiring notice and consent at the time of installation ignored the importance of a technique we refer to as "just in time" consent, which delays the notice and consent experience until the time most relevant to the user – just before the feature is executed. If a program crashes, for instance, Windows Error Reporting functionality will ask the user whether he or she would like to send crash information to

Microsoft. At this time, the user is able to examine the type of information that will be sent to Microsoft and to assess the actual privacy impact, if any, of transmitting such information in light of the potential benefit of receiving a possible fix for the problem. Presenting the notice and choice experience for Windows Error Reporting at the time Windows is first installed, in contrast, would lack this critical context.

As a result of cooperation between Congress and industry, the current version of the bill allows for "just in time" consent. This is an important inclusion that empowers users by providing them with notice and requiring choice at the time most appropriate to making an informed decision.

Unrealistic Uninstall Requirements. Finally, we were concerned about provisions in the bill that required standardized uninstall practices for all software, which we feared would be unworkable in many circumstances. For example, there are cases where a full and complete uninstall is neither technically possible nor desirable, such as with a software component that is in use and shared by other programs. In addition, there are other cases where an uninstall may be technically possible, but the cost to provide such functionality would be prohibitive, such as with complex software systems that may require the entire software system to be removed. Finally, there are situations where requiring uninstall could actually compromise the security of the system, such as backing out security upgrades or removing critical services.

Here again, the Committee has been responsive to industry concerns, and the bill has been modified to provide legitimate developers with the flexibility necessary to avoid

the types of problems outlined above. We look forward to continuing to work with the Committee to ensure that all appropriate uninstall scenarios are adequately addressed.

Legislation Must Be Forward-Thinking.

As Chairman Barton rightly recognized when bringing the SPY ACT to the House floor last term, "technological development moves quickly, much faster than the regulatory or legislative process."[7] We praise the Chairman for his hard work to move the SPY ACT through the legislative process so we can rapidly get additional tools in the hands of regulators to fight this burgeoning threat. But spyware is a relatively new problem, and the list of acts prohibited by the bill today might not capture every practice used by bad actors tomorrow. We and others in the industry are working to develop and implement new and better anti-spyware tools that will empower consumers to make more informed choices with respect to their computers. We need to make sure that the law does not create disincentives for consumers to use these tools, or for companies to develop and distribute them.

Congress recognized the importance of enabling consumers to take advantage of technological tools in addressing spam. In that context, Congress worked to clarify that merely because a message is not unlawful under federal law does not mean that consumers are in any way precluded from using technology to block the message. Similarly, with respect to spyware, simply because a software program complies with the SPY ACT should not prohibit consumers from choosing whether to download it, nor

---

[7] 150 Cong. Rec. H8080-81 (daily ed. Oct. 5, 2004) (statement of Rep. Barton).

should it leave vendors of anti-spyware tools open to legal action for providing tools that enable consumers to make these choices. We think it is self-evident that the SPY ACT should support the creation of such tools and not provide disincentives for the development of ever more powerful anti-spyware technologies. We look forward to working with Congress to ensure that the legislation achieves its aims of empowering consumers to maintain control over their computer systems and protect themselves as they see fit.

* * *

We want to thank the Committee once again for your attention to the spyware problem and for extending Microsoft an invitation to share our ideas and experiences with you – both today and as this process moves forward. By continuing to attack the problem on several levels – consumer education, technology solutions, industry best practices, aggressive enforcement, and targeted legislation – we believe we can thwart the efforts of those who produce and distribute spyware. Microsoft remains committed to working with you to prevent bad actors from deceiving consumers and destroying their computing experience.